anand guru

SOC EXPERTS

Interview Questions on
Logs (Raw Logs)

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What are the different logging levels in network devices?

Most network device have the following logging levels

- Level 0 —**Emergency** : System unusable
- Level 1 — **Alert** : Immediate action needed
- Level 2 — **Critical** : Critical condition—default level
- Level 3 — **Error** : Error condition
- Level 4 — **Warning** : Warning condition
- Level 5 — **Notification** : Normal but significant condition
- Level 6 — **Informational**: Informational message only
- Level 7 — **Debugging** : Appears during debugging only

anand guru

What are the important logs in Windows Server?

Windows Event Logs are the most important logs in Windows servers.

There are 3 main categories in Windows Event Logs

- **Application**
- **System**
- **Security**

Default location of logs for few log sources.

Windows Event Logs : C:\WINDOWS\system32\config\

Windows DHCP : C:\Windows\System32\DHCP

Windows DNS : **(Trick Question)** By default DNS logging is not enabled. When we enable we get an option to choose the log file path

Linux System : /var/log/messages

Exchange Mail Server : %ExchangeInstallPath%\TransportRoles\Logs\MessageTracking NOTE: Important logs in Exchange are Message Tracking logs

anand guru

Can you recall few Event IDs of Windows Event Logs?

1. 4624 – Successful User Account Login
2. 4625 – Failed User Account Login
3. 4720 – A user account is created
4. 4726 – A user account was deleted
5. 4740 – A user account was locked out
6. 4767 – A user account was unlocked
7. 1102 – The audit log was cleared

anand guru

What are Windows Logon Types?

The logon type field indicates the kind of logon that occurred.

Logon Type 2 – Interactive

Logon Type 3 – Network

Logon Type 4 – Batch

Logon Type 5 – Service

Logon Type 7 – Unlock

Logon Type 8 – NetworkCleartext

Logon Type 9 – NewCredentials

Logon Type 10 – RemoteInteractive

Logon Type 11 – CachedInteractive

Logon type 2, 3 & 10 are the most common type of logons

What are the reasons for Login failures in Windows?

Status and Sub Status Codes	Description
0xC0000064	User name does not exist
0xC000006A	User name is correct but the password is wrong
0xC0000234	User is currently locked out
0xC0000072	Account is currently disabled
0xC000006F	User tried to logon outside his day of week or time of day restrictions
0xC0000070	Workstation restriction, or Authentication Policy Silo violation
0xC0000193	Account expiration
0xC0000071	Expired password
0xC0000133	Clocks between DC and other computer too far out of sync
0xC000015B	The user has not been granted the requested logon type (aka logon right) at this machine

What are the important fields in antivirus logs?

Date & Time	- 18 Feb 2020 10:10:48
Host	- LJOHN0708
IP Address	- 10.10.2.78
User	- ABCInsurance\john
File Name	- goodmovie.exe
File Path	- D:\Movies\New Folder\goodmovie.exe
Malware Name	- Every vendor has their naming conventions
Malware Category	- Trojan, Worm, Ransomware etc.
Action Taken by AV	- Clean, Delete, Quarantine, Failed to Clean, Failed to delete, Failed to Quarantine

What are the important fields in firewall logs?

Date & Time

Source IP

NAT Source IP

Source Port

Source Interface/Zone

Destination IP

NAT Destination IP

Destination Port

Destination Interface/Zone

Rule Name

Action

Bytes Sent

Bytes Received

Source Country

Destination Country

anand guru

What are the important fields in IPS logs?

Date & Time

Source IP

Source Port

Destination IP

Destination Port

Attack Name

Attack Severity

Source Country

Destination Country

Action

anand guru

What are the important fields in proxy logs?

Date & Time

Source IP

User

URL

Domain

Website Category

Action

Bytes Sent

Bytes Received

anand guru

What are the important fields in WAF logs?

Date & Time

Client IP

Request Headers

Response Headers

URL

Referrer

Method

HTTP Status Code

Attack Type

Attack Severity

anand guru

What logs do you pull from AWS?

AWS CloudTrail Logs

AWS CloudWatch Logs

How do you pull logs from AWS?

Using AWS API.

We would need the **Access key** and **Secret access key** of a user account. This user should have permission to read logs form S3 buckets.

What logs do you collect from a database?

Audit Logs

Why do we need raw logs?

- The raw logs are required for Forensics and Compliance purposes.

Difference between Flows and Events.

- **Event** is a log of a particular action.
- A **flow** records information like number of packets, bytes sent, bytes received and connection time.

Difference between an Event, Alert and Incident

- **Event** is a log of particular action on a server.
- **Alert** is a suspicious (not confirmed) activity in the network.
- An **incident** is a confirmed malicious activity.